

REMARKS

In the Office Action dated May 30, 2007, claims 1-6 were rejected. Claims 1-6 are now pending in the application. In view of the remarks and amendments, Applicant respectfully requests reconsideration of the application.

Claims 1-3, 5 and 6 were rejected under 35 U.S.C. § 102(e) as being anticipated by the Medvinsky reference (US Publication No. 20030093694).

For Claim 1 reciting the portion "wherein the encrypted data packet is a same size as the original data packet", the Examiner relies on paragraph [0105] of the Medvinsky reference to show that the AES is utilized. Further, the Examiner states that a characteristic of stream/block ciphers makes them suitable for applications that require the encrypted cipher text data be the same size as the original plaintext data.

Applicant respectfully disagrees with the Examiner's assertion that by utilizing AES, the stream cipher mode is implicated. Instead, paragraph [0105] of the Medvinsky reference indicates that AES is utilized as a block cipher in CBC mode.

Notwithstanding, Applicant has amended Claim 1 to include the limitation, in part, of:

wherein the modified header ~~encrypted data packet~~ is
a same size as the original header ~~data packet~~.

In marked contrast to the Medvinsky reference, the invention as described in Claim 1 states that the modified header is the same size as the original header. The Medvinsky reference teaches prepending fields to the original encrypted RTCP packet. (Medvinsky, paragraph [0099]) For example, the Medvinsky

reference teaches use of 4 additional fields (session ID, packet sequence number, initialization vector, and message authentication code). (Medvinsky, paragraphs [0100-0103]) Claim 1 includes the limitation that the modified header is the same size as the original header. The Medvinsky reference teaches away from Claim 1 by adding additional fields to the RTCP packet.

Independent Claim 6 is allowable for the same reason as discussed above.

Claims 2, 3, and 5 depend directly or indirectly on allowable independent Claim 1 and, therefore, are patentable for at least the same reasons discussed above.

Claim 4 was rejected under 35 U.S.C. § 103(a) as being unpatentable over the Medvinsky reference (US Publication No. 20030093694).


Claim 4 depends directly or indirectly on allowable independent Claim 1 and, therefore, is patentable for at least the same reasons discussed above.

In view of the foregoing remarks and amendments, Applicant respectfully submits that all pending claims are in condition for allowance. Such allowance is respectfully requested.

If the Examiner finds any remaining impediment to the prompt allowance of these claims that could be clarified with a telephone conference, the Examiner is respectfully requested to contact Richard H. Butler at (408) 425-3376.

Respectfully submitted,

Dated: 9/29/07



Richard H. Butler
Registration No. 40,932

Please Send Correspondence to:
Valley Oak Law
5655 Silver Creek Valley Road
#106
San Jose, CA 95138
(408)425-3376